HIAC

🌐 Online Safety Guidance for Staff

High Impact Academic Coaching Ltd
89–90 Paul Street, London, EC2A 4NE
Company Number: 12386860
📧 safeguarding@highimpactacademiccoaching.com
🌐 www.highimpactacademiccoaching.com
Audience: All Staff
Owner: Designated Safeguarding Lead (DSL)

---

1. Purpose

This guidance supports staff in understanding their responsibilities for promoting and maintaining online safety. It outlines best practices, risk indicators, and reporting procedures to protect children and young people (C/YP) from harm in digital environments.

---

2. Safeguarding & Legal Context

Staff must be familiar with the following statutory frameworks:

- *Keeping Children Safe in Education (2024)*
- *Prevent Duty Guidance (2023)*
- *UK GDPR & Data Protection Act 2018*
- *Education Act 2002*
- *Children Act 1989 & 2004*

Online safety is a core safeguarding responsibility. Risks include:

- Cyberbullying
- Grooming and exploitation
- Exposure to extremist content
- Image-based abuse (e.g., sexting)
- Online hate and misinformation

---

3. Staff Responsibilities

All staff must:

- Model safe and respectful online behaviour
- Use only approved platforms for communication and teaching
- Maintain professional boundaries in digital interactions
- Report any online safety concerns to the DSL immediately
- Complete annual online safety and Prevent training
- Ensure learners understand how to stay safe online

---

4. Digital Conduct Expectations

- Do not use personal accounts or devices to contact learners
- Do not share confidential learner data via unsecured platforms
- Do not access or share inappropriate content
- Do not engage in political, religious, or personal debates with learners online
- Always log out of shared devices and lock screens when unattended

---

5. Online Teaching & Remote Learning

- Use only HIAC-approved platforms (e.g., Teams, Zoom, Google Classroom)
- Record sessions where appropriate and notify learners
- Maintain a professional environment (e.g., dress, background, tone)
- Ensure learners understand behaviour expectations during online sessions

---

6. Recognising Online Risks

Staff should be alert to signs such as:

- Sudden changes in online behaviour or mood
- Secretive use of devices
- References to unsafe apps, websites, or contacts
- Withdrawal from peer groups or learning
- Use of extremist language or ideologies

---

7. Reporting Procedures

- Concerns must be reported to the DSL immediately
- Use the HIAC Safeguarding Concern Form or speak directly to the DSL
- For serious incidents (e.g., grooming, radicalisation), the DSL may refer to:
    - Police
    - Channel Programme
    - Local Authority Designated Officer (LADO)
    - Children’s Social Care

---

8. Data Protection & Privacy

- Use encrypted platforms for storing and sharing learner data
- Do not photograph or record learners without consent
- Ensure devices are password-protected and regularly updated
- Follow HIAC’s Data Protection Policy at all times

---

9. Monitoring & Filtering

- HIAC uses filtering systems to block harmful content
- Monitoring tools detect inappropriate or risky behaviour
- Staff must not attempt to bypass filters or disable security settings

---

10. Support & Resources

Staff can access support and resources from:

- DSL and SLT
- National Online Safety (www.nationalonlinesafety.com)
- CEOP (www.ceop.police.uk)
- UK Safer Internet Centre (www.saferinternet.org.uk)

---

11. Review & Development

This guidance is reviewed annually or following any major incident. Staff feedback and safeguarding trends inform updates.

Year-on-Year Document Review

Review Date	Reviewer Name	Changes Made / Notes	Next Review Date
01/10/25	Kris Geddes	N/A	01/10/26